Secret Sharing

Henning Hontheim

10. März 2020

Inhaltsverzeichnis

1 Einleitung 1

1 Einleitung

Mehrere Wissenschaftler N arbeiten zusammen an einem Geheimprojekt. Um die Dokumente geheim zu halten und um Missbrauch vorzubeugen, verschließen sie diese in einem Tresor. Nur wenn mindestens die Hälfte aller Wissenschaftler anwesend ist, soll sich der Tresor öffnen lassen. Wie viele paarweise verschiedene Schlösser S muss der Tresor mindestens besitzen? Wie viele paarweise verschiedene Schlüssel s muss jeder Wissenschaftler mindestens bei sich tragen? Siehe [2] nach [1].

Beispiel 1.1. Sei $N = 11$ die Anzahl aller Wissenschaftler und $n = \lceil \frac{N}{2} \rceil = 6$ die Anzahl derer, die mindestens anwesend sein müssen, damit sich der Tresor öffnen lässt. Folglich muss es also für jede Teilmenge mit k Wissenschaftlern, wobei $k = N - n = 5$, genau ein Schloss geben, für das keiner der k Wissenschaftler einen Schlüssel besitzt. Also muss der Tresor $S = \binom{N}{k} = \binom{11}{5} = 462$ paarweise verschiedene Schlösser besitzen.

Sei $W = \{w_1, w_2, \dots w_k, w_{k+1}\}$ mit $|W| = k + 1 = 6$ die Menge von Wissenschaftlern, die mindestens benötigt wird, um den Tresor zu öffnen. Dann gibt es genau ein bestimmtes Schloss S', für das keiner der Wissenschaftler aus $W \setminus w_{k+1}$ einen Schlüssel besitzt, der Wissenschaftler w_{k+1} jedoch schon. Da für jede Permutation von $k = 5$ Wissenschaftlern genau der w_{k+1} existiert, der die Teilmenge W „vervollständigt“, bekommt jeder Wissenschaftler $s = \binom{N-1}{|W|-1} = \binom{N-1}{k} = \binom{10}{5} = 252$ Schlüssel. Das ergibt eine Gesamtanzahl an $11 \cdot 252 = 2772$ Schlüsseln. Dass dies keine praktikable Lösung des Problems ist, ist offensichtlich.

Literaturverzeichnis

[1] Liu, C. L. *Introduction to Combinatorial Mathematics*. McGraw-Hill, New York, 1968.

[2] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (Nov 1979), 612–613.